SPAWAR PD16
Information and
Electronic Warfare

Industry Partnership Conference

25 June 1997

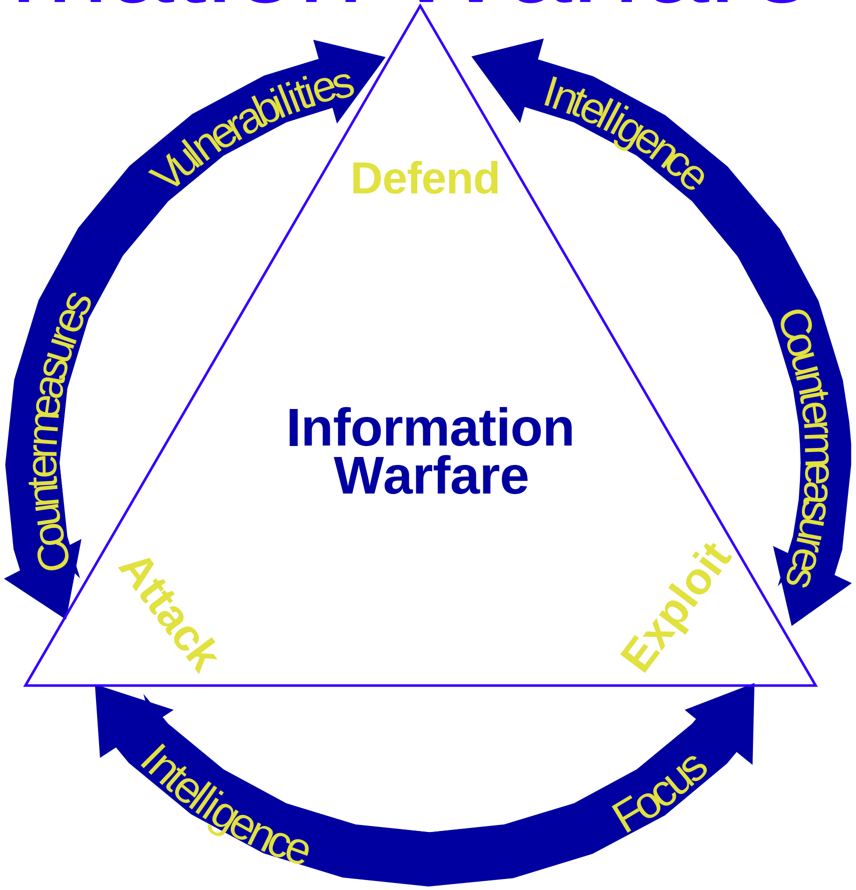
By: CAPT M. A. Shupack
PD16 (Acting)

Agenda

- PD 16 Opening Remarks
  - Introduction of Panel
  - Direction for Navy Information Warfare (IW)
- PD 16 Mission/Organization
- IW Elements
  - Nature of Work
  - Upcoming Opportunities
  - Planned Procurements
- Field Activity Remarks
- PD 16 POCs

Industry Partnership
SPAWAR
'97

Information Warfare (IW)



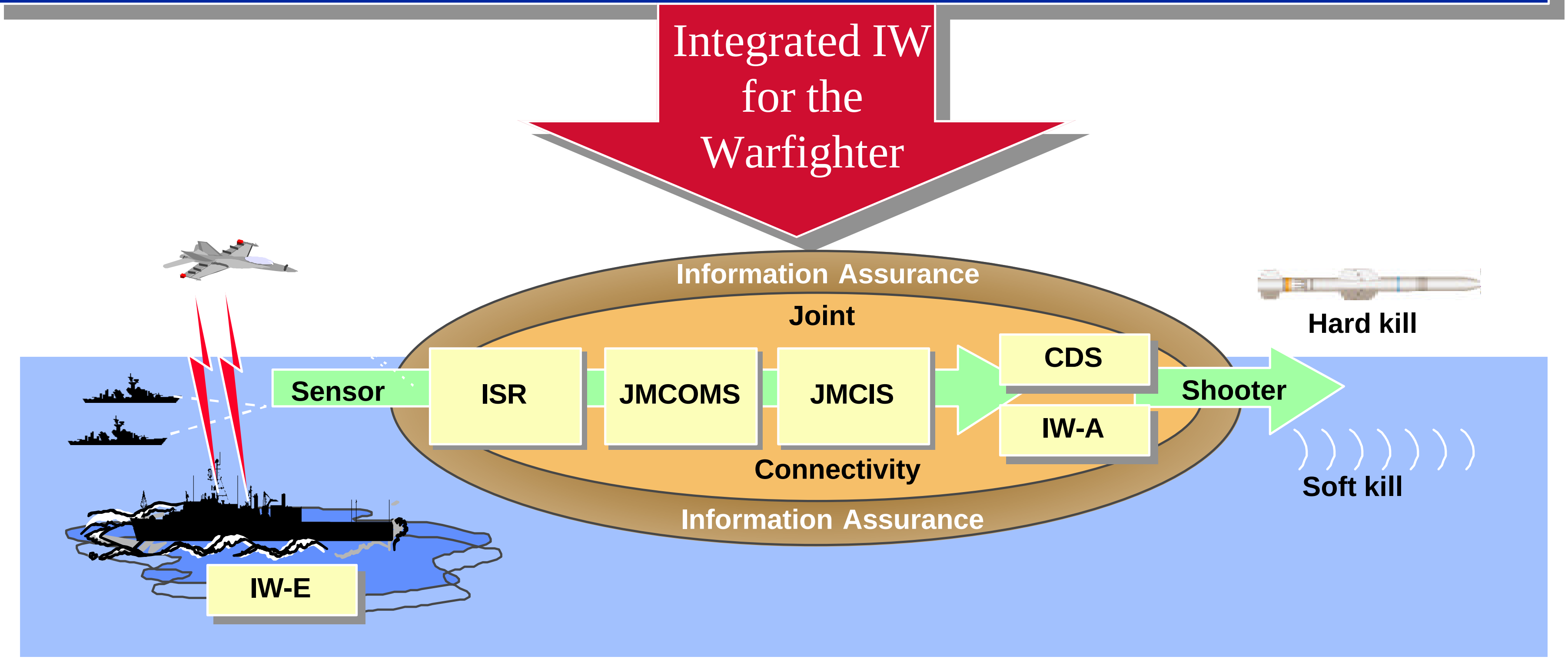
- Information Superiority - The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.*

(* From Joint Vision 2010 - GEN John M. Shalikashvili
Chairman, Joint Chiefs of Staff)

Current and Future Warfighting Environment

The Historical Legacy

Historically, IW “Attack” and “Defend” Capabilities Have Been Adhoc, Fragmented and Under-Funded. Shipboard IW Capabilities Have Focused On Passive Exploitation of Threat Communications and Own-Force Protection.



Integrated IW for the Warfighter

Information Assurance

Joint

Sensor

ISR

JMCOMS

JMCIS

CDS

IW-A

Shooter

Connectivity

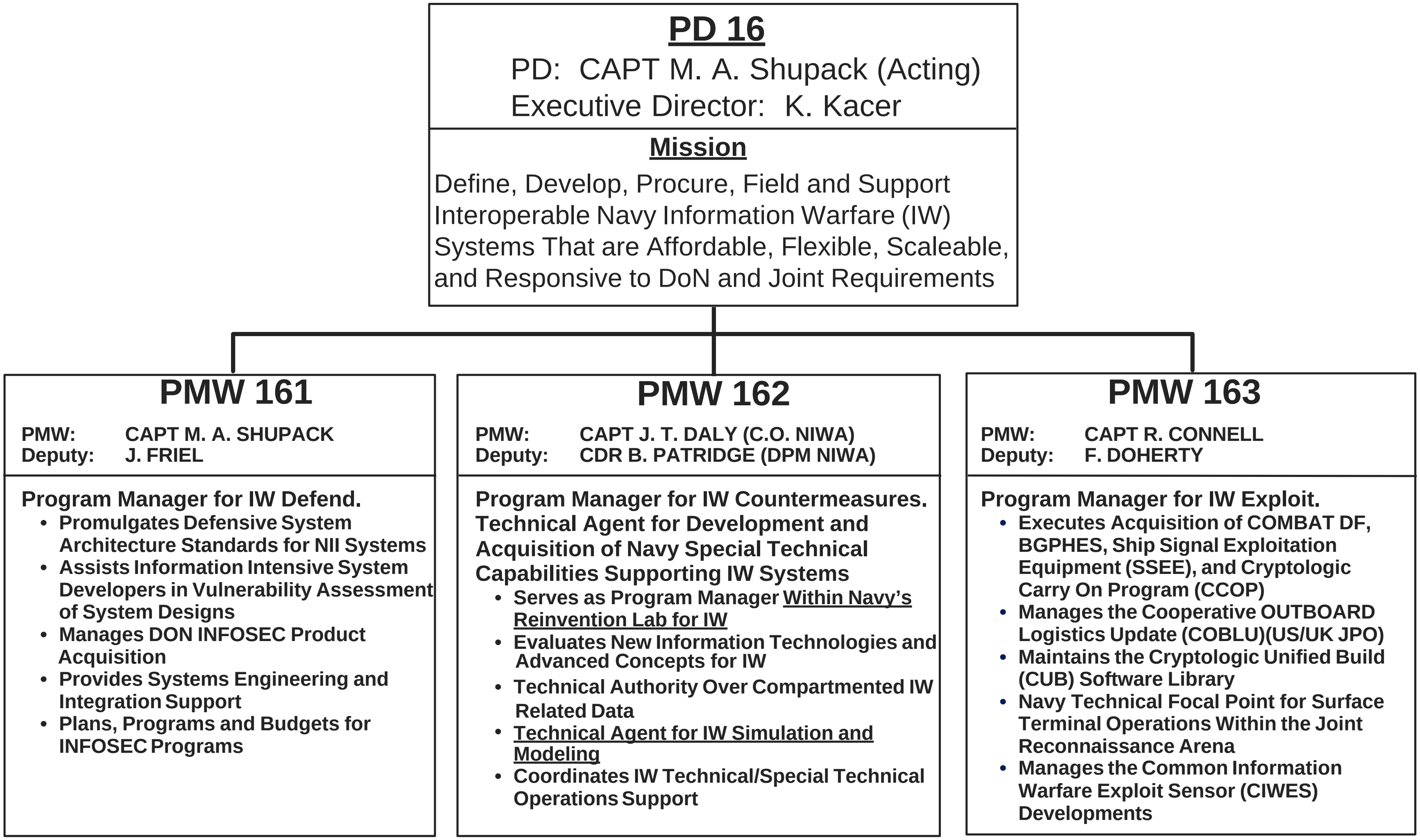
Information Assurance

IW-E

Hard kill

Soft kill

PD 16 Mission/Organization



PD 16

PD: CAPT M. A. Shupack (Acting)
Executive Director: K. Kacer

Mission

Define, Develop, Procure, Field and Support Interoperable Navy Information Warfare (IW) Systems That are Affordable, Flexible, Scaleable, and Responsive to DoN and Joint Requirements

PMW 161

PMW: CAPT M. A. SHUPACK
Deputy: J. FRIEL

Program Manager for IW Defend.

- Promulgates Defensive System Architecture Standards for NII Systems
- Assists Information Intensive System Developers in Vulnerability Assessment of System Designs
- Manages DON INFOSEC Product Acquisition
- Provides Systems Engineering and Integration Support
- Plans, Programs and Budgets for INFOSEC Programs

PMW 162

PMW: CAPT J. T. DALY (C.O. NIWA)
Deputy: CDR B. PATRIDGE (DPM NIWA)

Program Manager for IW Countermeasures. Technical Agent for Development and Acquisition of Navy Special Technical Capabilities Supporting IW Systems

- Serves as Program Manager Within Navy's Reinvention Lab for IW
- Evaluates New Information Technologies and Advanced Concepts for IW
- Technical Authority Over Compartmented IW Related Data
- Technical Agent for IW Simulation and Modeling
- Coordinates IW Technical/Special Technical Operations Support

PMW 163

PMW: CAPT R. CONNELL
Deputy: F. DOHERTY

Program Manager for IW Exploit.

- Executes Acquisition of COMBAT DF, BGPHES, Ship Signal Exploitation Equipment (SSEE), and Cryptologic Carry On Program (CCOP)
- Manages the Cooperative OUTBOARD Logistics Update (COBLU)(US/UK JPO)
- Maintains the Cryptologic Unified Build (CUB) Software Library
- Navy Technical Focal Point for Surface Terminal Operations Within the Joint Reconnaissance Arena
- Manages the Common Information Warfare Exploit Sensor (CIWES) Developments

Industry Partnership
SPAWAR
'97

Acquisition Strategy

- Build a little
- Test a little
- Field a **LOT**

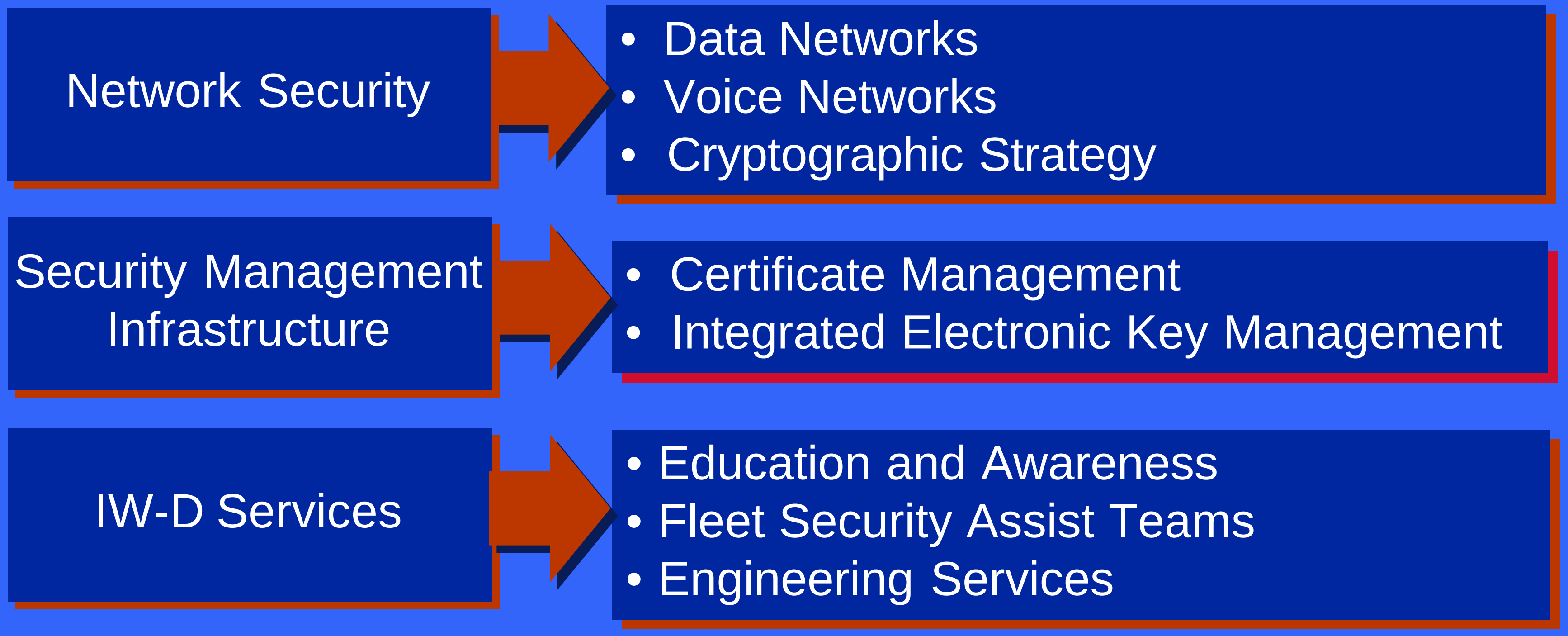
Evolutionary, stepwise, incremental approach to system development utilizing COTS, GOTS and NDI in a totally open, interoperable, global architecture.

Industry Partnership
SPAWAR
'97

SPAWAR PMW 161

Information Warfare-Defend (IW-D)

IW-D Current Focus



Network Security

- Data Networks
- Voice Networks
- Cryptographic Strategy

Security Management Infrastructure

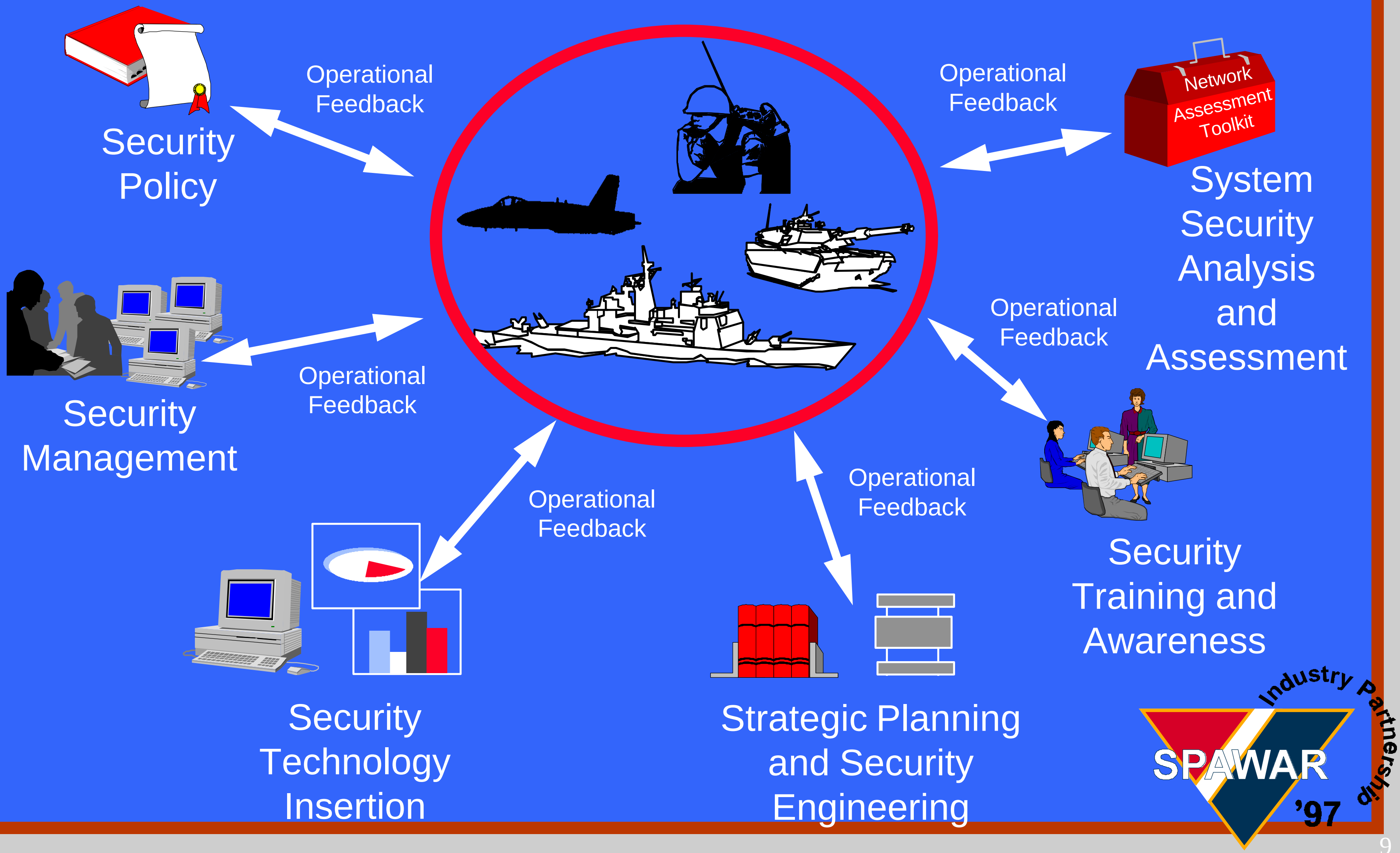
- Certificate Management
- Integrated Electronic Key Management

IW-D Services

- Education and Awareness
- Fleet Security Assist Teams
- Engineering Services

- **Deliver Affordable, Interoperable, Transparent, Effective and Supportable Security to the Warfighter**
- **Use Innovative Acquisition Strategies to Reduce Cost and Time to Fleet (Migrate from Uniquely Developed Security Products to COTS Technology)**

Interrelationships in IW-D



Security Policy

Operational Feedback

Security Management

Operational Feedback

Security Technology Insertion

Operational Feedback

Strategic Planning and Security Engineering

Operational Feedback

Security Training and Awareness

Operational Feedback

System Security Analysis and Assessment

Operational Feedback

Industry Partnership SPAWAR '97

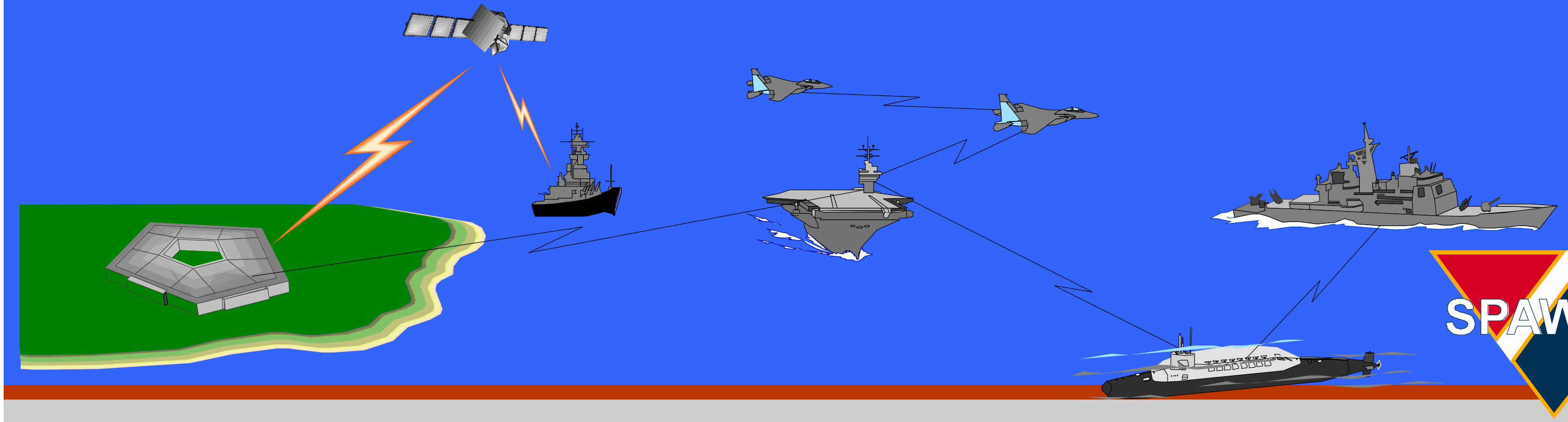
IW-D Solutions Sought

- Display Drivers to Show and Manage the IW-D “Picture” for an IW Officer
- Decision Aids to Enable the IW Officer to Manage Systems that are Attacked or Threatened
- Low Overhead Technology to Manage Multiple Security Domains on Shared Military Systems
- Inexpensive, Programmable Cryptography with no Host Certification Requirements (“Plug & Play”)
- Graphical Design/Risk-Analysis Tools to Show System Architecture, Threat Scenarios and Countermeasures
- Software Production Engines that can Code Trusted Software Modules Directly from Hi-Level Requirements

Industry Partnership
SPAWAR
’97

Industry Opportunities -- Goals for Industry

- Develop and Provide Solutions Compliant With Open System Architectures and Standards
  - Technical Architecture for Information Management (TAFIM)
  - Defense Information Infrastructure (DII) Common Operating Environment (COE)
  - Joint Technical Architecture (JTA)
- Maximize Use of NDI and COTS Products; Software and Hardware Integration Services are Key; Employ Solutions From Other Services, NSA, DISA, and Allies to Foster Interoperability



SPAWAR Industry Partnership '97

Industry Opportunities -- Acquisition Strategy

- Commercial Technology Purchased Through IDIQ, Umbrella, and General Schedule Contracts

- IW-D Non-Developmental Items (NDI) Obtained Through Cooperation with the National Security Agency and Other Services

- Competitive Procurements When Required for Specialized Products and Systems and for Engineering, Integration, and Support Services

SPAWAR PMW 162/NIWA

Information Warfare-Attack (IW-A)

Industry Partnership SPAWAR '97

IW-A Mission

- The Mission of the Naval Information Warfare Activity (PMW 162) is to Assess, Adapt, Develop, Prototype, Demonstrate, Selectively Acquire, Apply and Test <u>Advanced Information System Technologies</u> in Support of Requirements for IW. (NSGINST 5450.65)

Industry Partnership SPAWAR '97

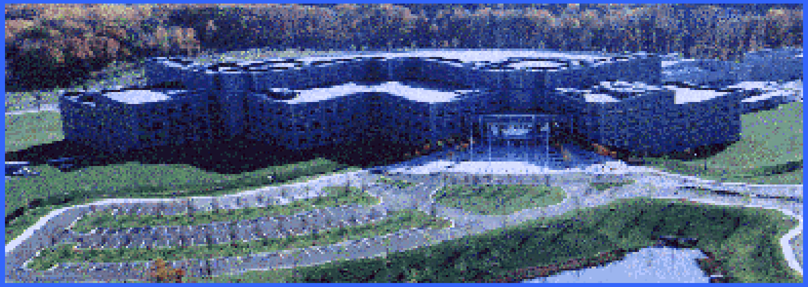
IW-A Functions

- Navy's (OPNAVINST 3430.26) Technical Agent For IW:
  - Navy Vulnerability Assessment Program for IW-D
  - RDTE&A for Offensive IW Capabilities for IW-A
  - Technology Evaluation, Modeling and Simulation (e.g., Radio Frequency Mission Planner) for IW-E

Industry Partnership SPAWAR '97

IW-A Multi-Disciplinary Approach for IW Technical Development

- NIWA (PMW 162) Draws Technology Support From:
  - NSA/USCS
  - Navy Tech Base/Lab System
- NIWA (PMW 162) is Organized For:
  - Technical Threat Analysis and <u>Vulnerability Assessment</u>
    - Based on All-source Intelligence
  - Development and Acquisition of <u>Special Technical Capabilities</u>
    - Rapid Prototyping Now
    - Just-in-time Approaches in Future



IW Reinvention Laboratory

- Concept: NIWA (PMW 162) Designated as a Reinvention Laboratory for IW Under the National Performance Review
- Purpose: Facilitate Pilot Project/Rapid Prototype Approach to IW
  - Timely Response to the Information Technology Revolution and Commercial Innovation
- Implementation:
  - Execute With Streamlined Acquisition Approach
    - Advanced Technical Development Program Documentation and Standards
  - Rely Upon COTS/GOTS Technology Base
    - Integrated Via NRL “Skunkworks”
    - Supported by National Labs, FFRDCs and Select Vendors
  - Use In-house Vulnerability Assessments to Track Technology/Targets and Drive Prototype Development
    - Comprehensive Access to Sensitive Sources and Methods (NSA/CIA/DIA)
    - All-source Analysis

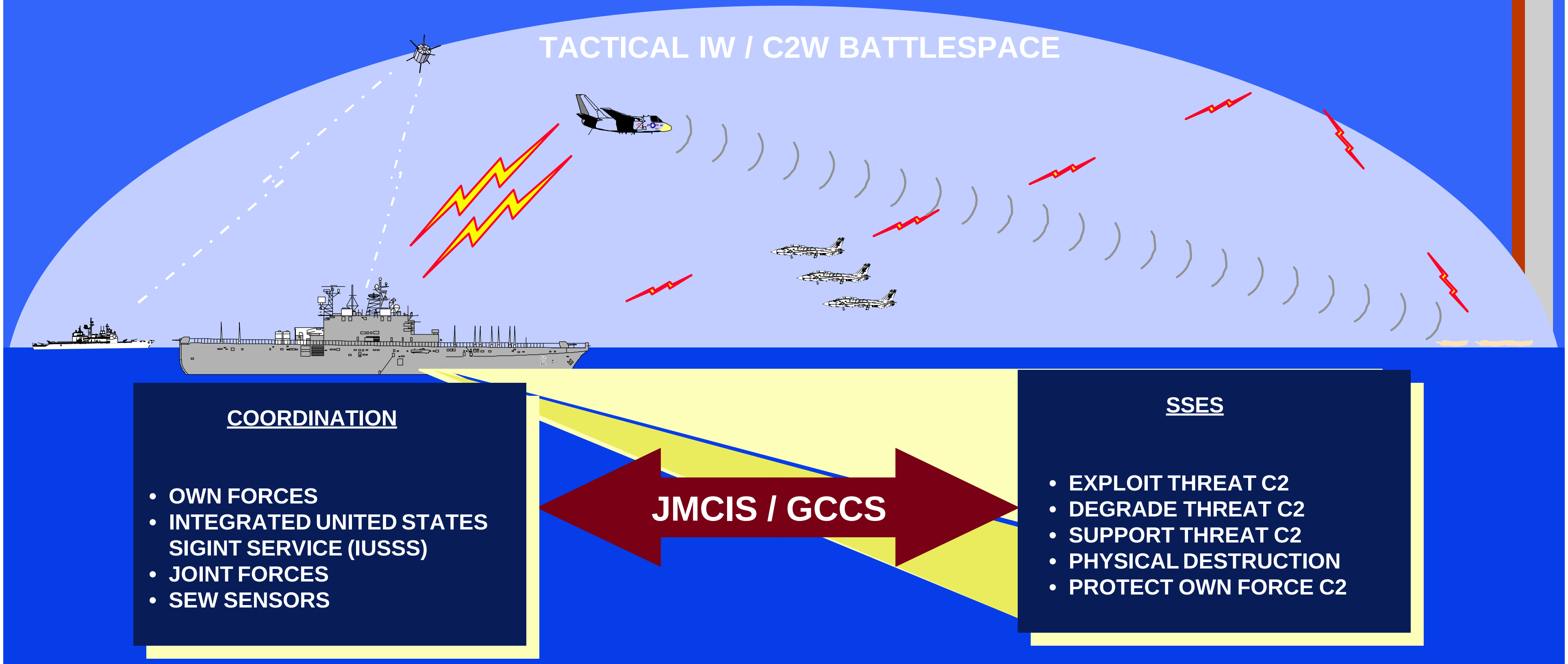
IW-A Guidelines

- Don’t Try to Cover Every Possible Target
- Adopt a Modified “Just in Time” Prototype Approach
  - Point Designs of Capabilities Against Obvious Targets
- Rapid Prototyping Mechanism for Emergent Targets
  - NIWA (PMW 162) Intelligence Analysis Team
  - NIWA (PMW 162) Vulnerability Analysis Team

SPAWAR PMW 163

Information Warfare-Exploit (IW-E)

IW-E Concept



TACTICAL IW / C2W BATTLESPACE

COORDINATION

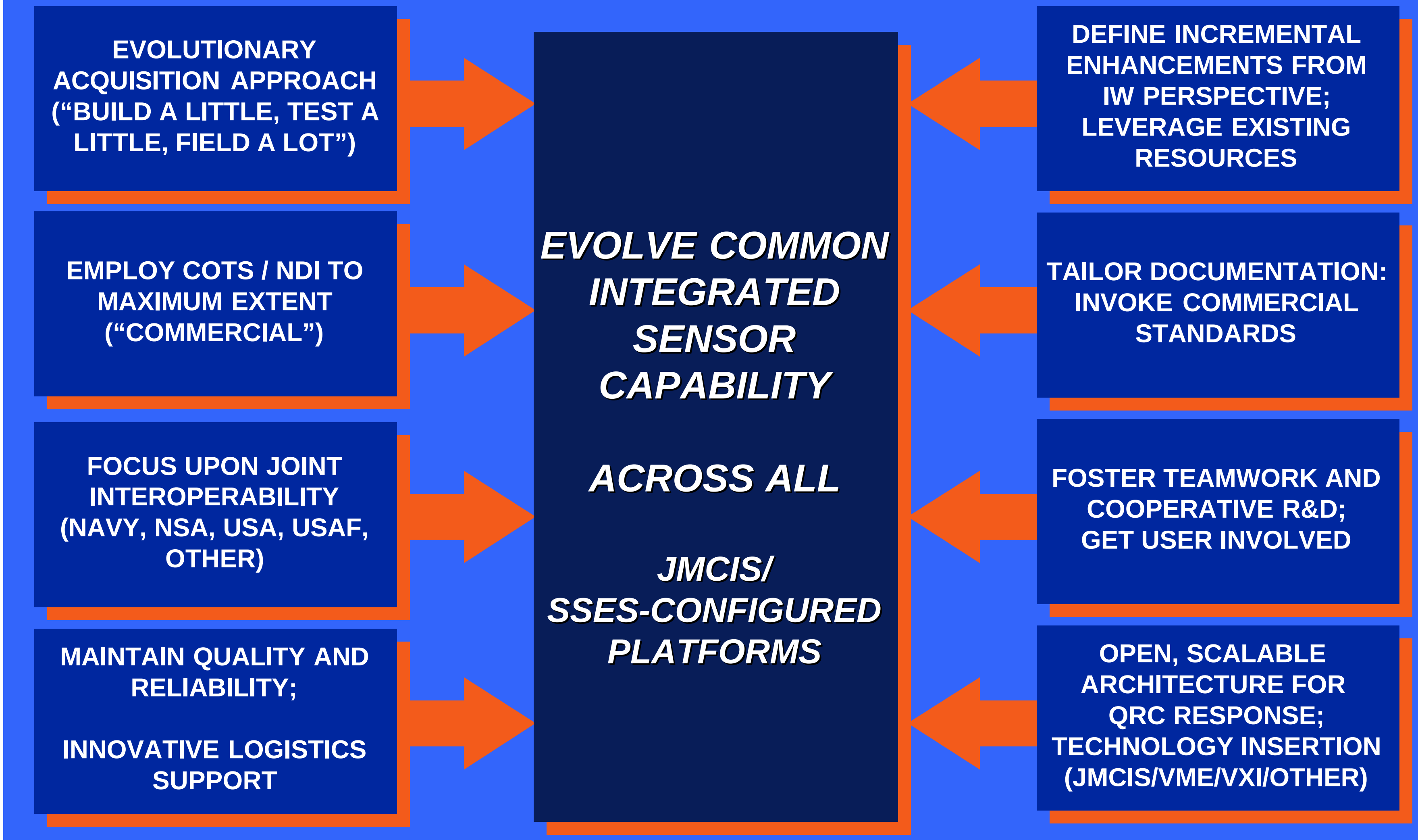
- OWN FORCES
- INTEGRATED UNITED STATES SIGINT SERVICE (IUSSS)
- JOINT FORCES
- SEW SENSORS

JMCIS / GCCS

SSES

- EXPLOIT THREAT C2
- DEGRADE THREAT C2
- SUPPORT THREAT C2
- PHYSICAL DESTRUCTION
- PROTECT OWN FORCE C2

IW-E Current Focus



EVOLUTIONARY ACQUISITION APPROACH (“BUILD A LITTLE, TEST A LITTLE, FIELD A LOT”)

EMPLOY COTS / NDI TO MAXIMUM EXTENT (“COMMERCIAL”)

FOCUS UPON JOINT INTEROPERABILITY (NAVY, NSA, USA, USAF, OTHER)

MAINTAIN QUALITY AND RELIABILITY;

INNOVATIVE LOGISTICS SUPPORT

EVOLVE COMMON INTEGRATED SENSOR CAPABILITY

ACROSS ALL

JMCIS/ SSES-CONFIGURED PLATFORMS

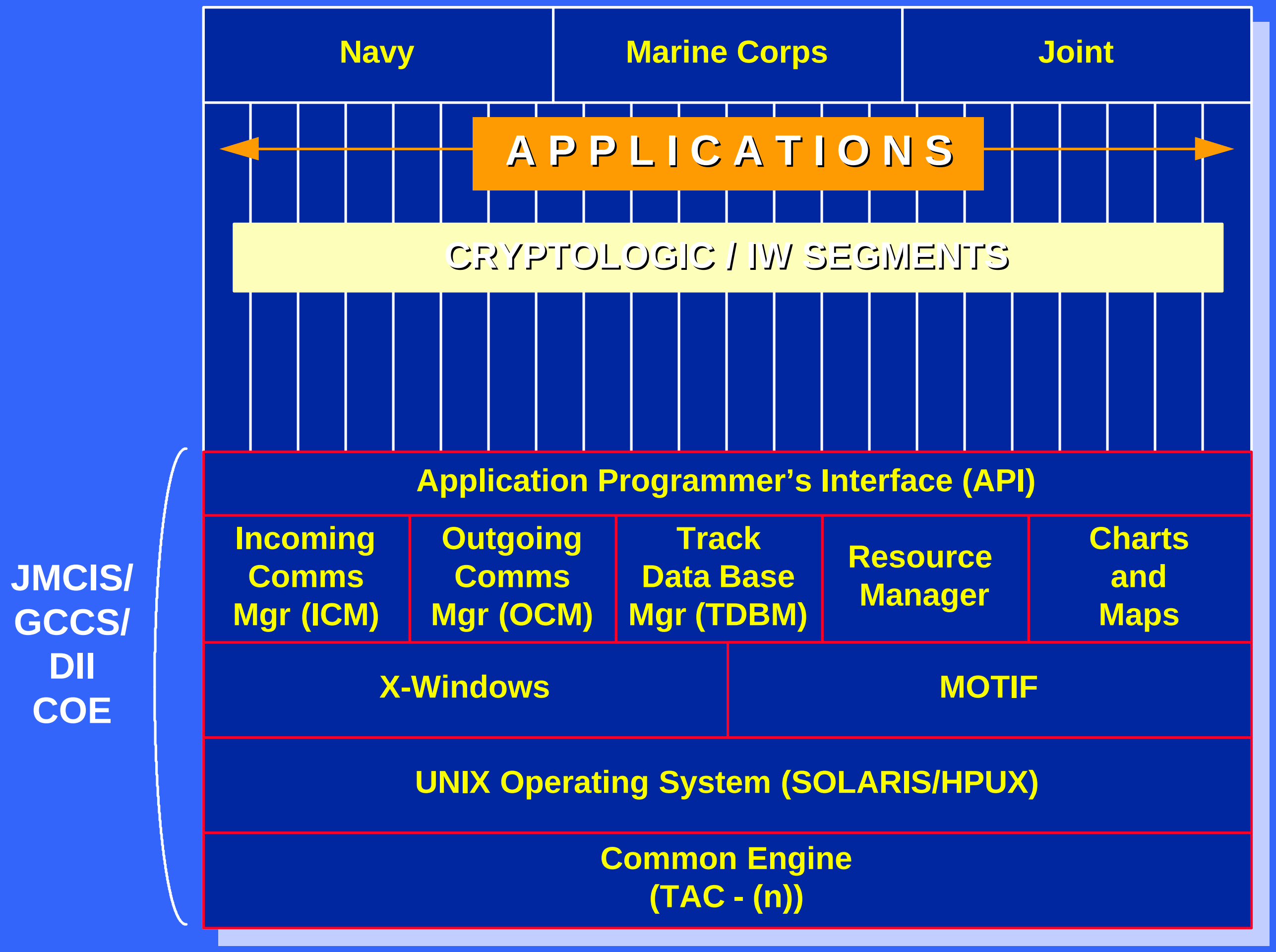
DEFINE INCREMENTAL ENHANCEMENTS FROM IW PERSPECTIVE; LEVERAGE EXISTING RESOURCES

TAILOR DOCUMENTATION: INVOKE COMMERCIAL STANDARDS

FOSTER TEAMWORK AND COOPERATIVE R&D; GET USER INVOLVED

OPEN, SCALABLE ARCHITECTURE FOR QRC RESPONSE; TECHNOLOGY INSERTION (JMCIS/VME/VXI/OTHER)

IW-E Software Architecture



Navy | Marine Corps | Joint

APPLICATIONS

CRYPTOLOGIC / IW SEGMENTS

Application Programmer's Interface (API)

Incoming Comms Mgr (ICM) | Outgoing Comms Mgr (OCM) | Track Data Base Mgr (TDBM) | Resource Manager | Charts and Maps

X-Windows | MOTIF

UNIX Operating System (SOLARIS/HPUX)

Common Engine
(TAC - (n))

JMCIS/
GCCS/
DII
COE

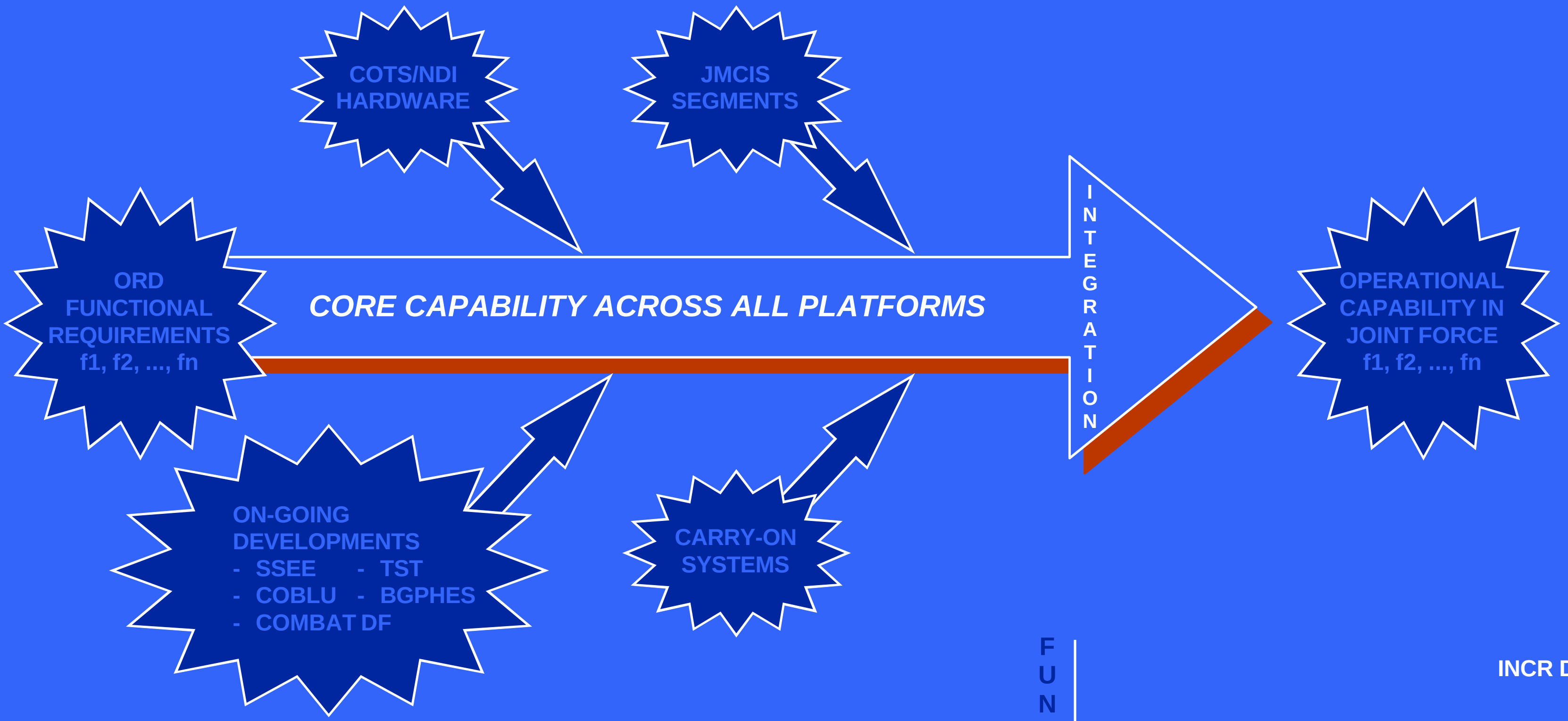
Standards

IEEE 802.3
POSIX
GOSIP
API
FDDI
DODHS
TAFIM
etc.

CRYPTOLOGIC / IW SEGMENTS ARE KNOWN AS
CRYPTOLOGIC UNIFIED BUILD (CUB)

Industry Partnership
SPAWAR
'97

IW-E Evolution Strategy



COTS/NDI HARDWARE

JMCIS SEGMENTS

ORD FUNCTIONAL REQUIREMENTS f1, f2, ..., fn

CORE CAPABILITY ACROSS ALL PLATFORMS

INTEGRATION

OPERATIONAL CAPABILITY IN JOINT FORCE f1, f2, ..., fn

ON-GOING DEVELOPMENTS
- SSEE
- TST
- COBLU
- BGPHES
- COMBAT DF

CARRY-ON SYSTEMS

n CONCENTRATE ON COMMERCIAL STANDARDS

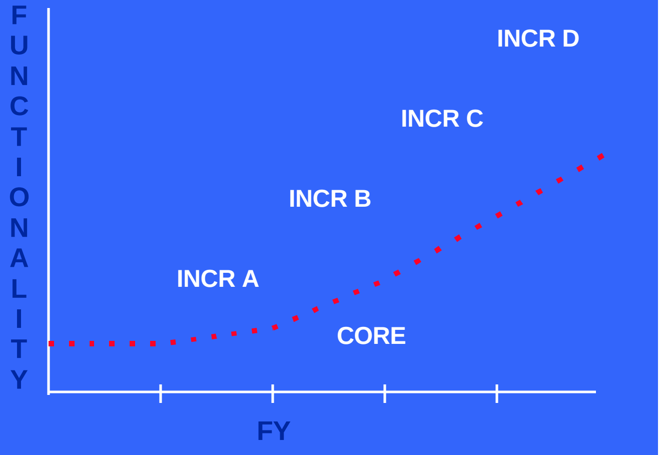
n OPEN ARCHITECTURE FOUNDATION

n REUSE JOINT AND TACTICAL SIGINT TECHNOLOGY (TST) EFFORTS

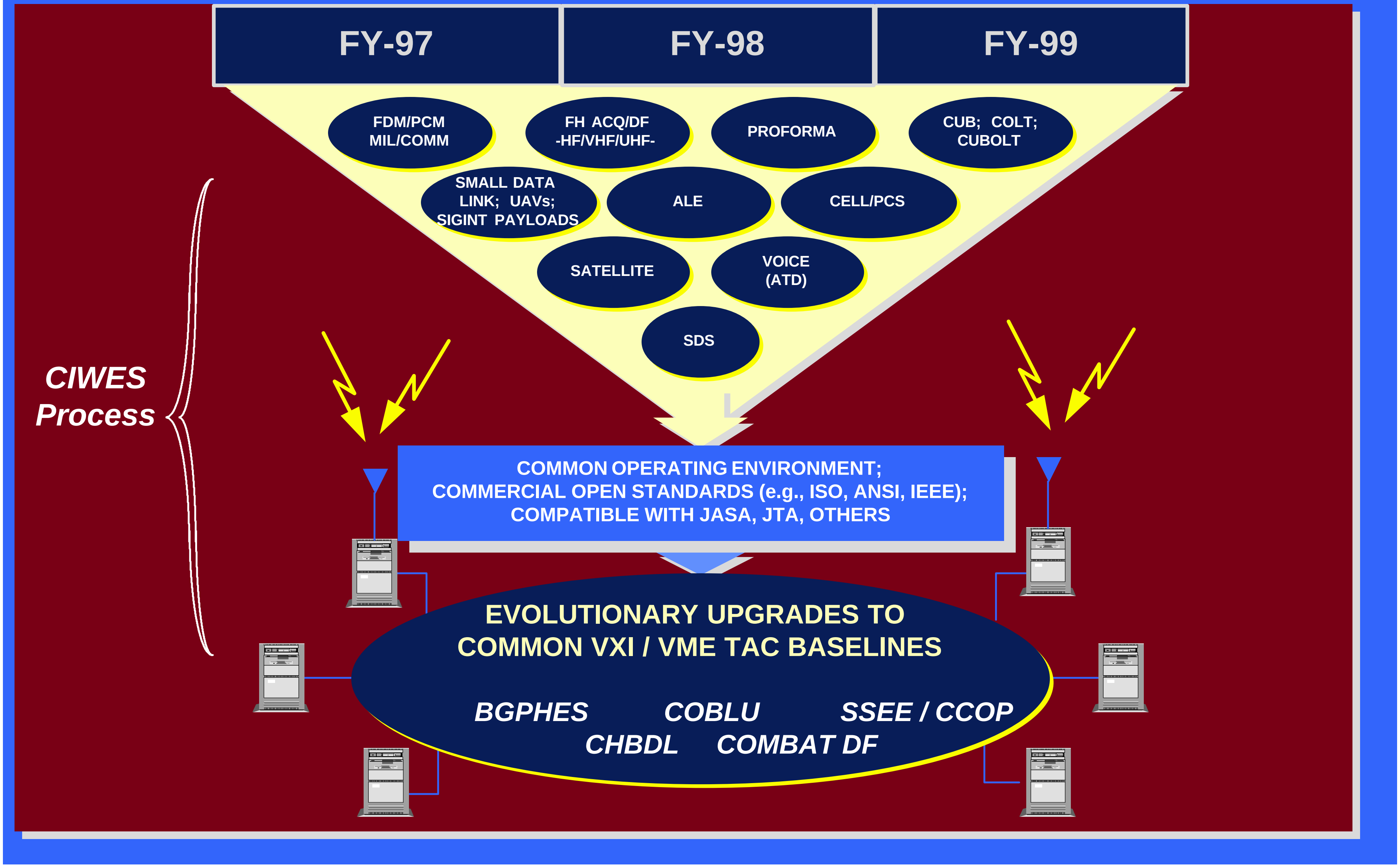
n INVOLVE CUSTOMER IN PROTOTYPING EFFORTS

n ESTABLISH CRITICAL INFRASTRUCTURE MASS FOR INTEGRATIONS

n DEFINE SYSTEM BASELINE ECPs



CIWES Concept



FY-97

FY-98

FY-99

FDM/PCM MIL/COMM

FH ACQ/DF -HF/VHF/UHF-

PROFORMA

CUB; COLT; CUBOLT

SMALL DATA LINK; UAVs; SIGINT PAYLOADS

ALE

CELL/PCS

SATELLITE

VOICE (ATD)

SDS

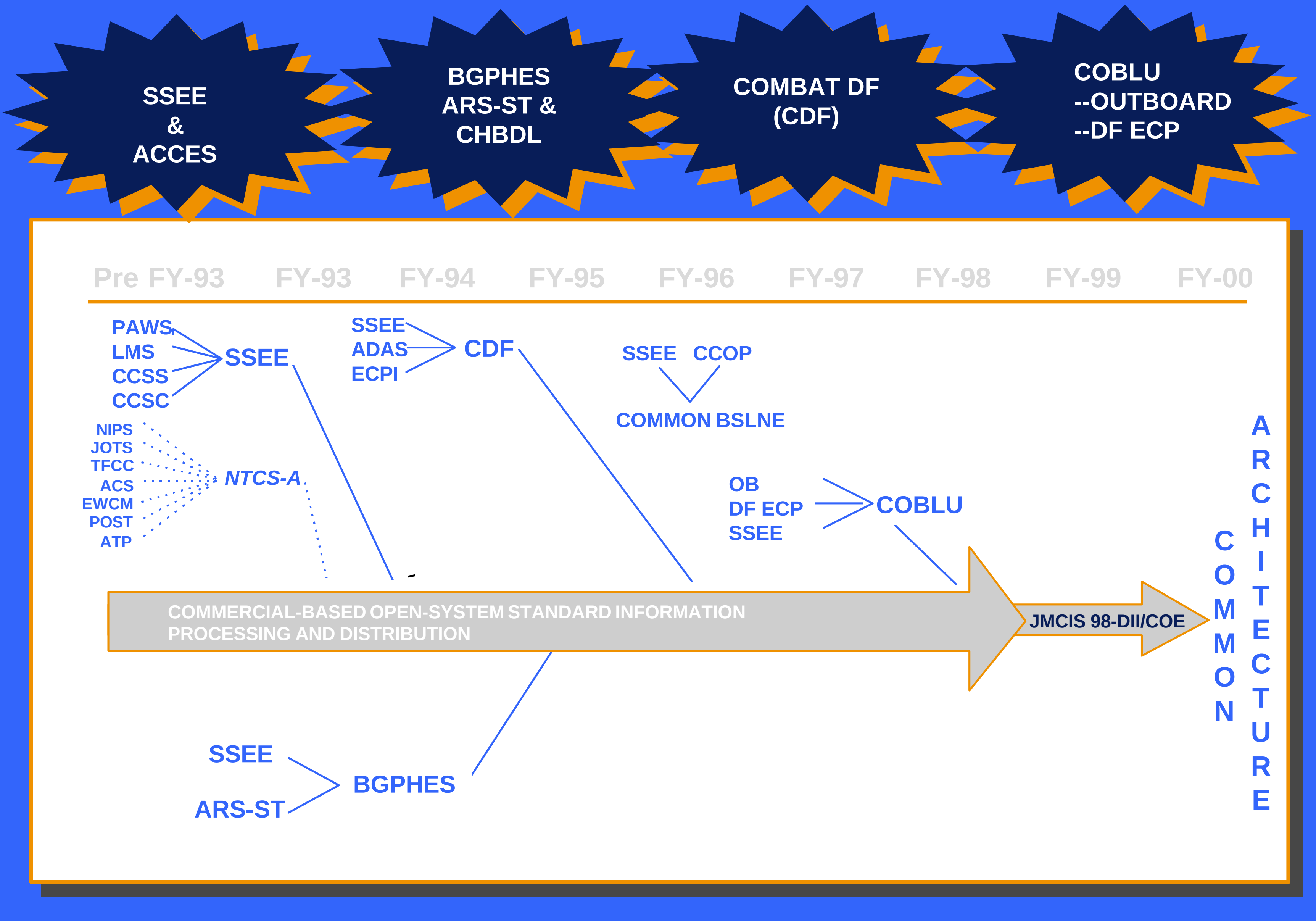
CIWES Process

COMMON OPERATING ENVIRONMENT;
COMMERCIAL OPEN STANDARDS (e.g., ISO, ANSI, IEEE);
COMPATIBLE WITH JASA, JTA, OTHERS

EVOLUTIONARY UPGRADES TO
COMMON VXI / VME TAC BASELINES

BGPHES *COBLU* *SSEE / CCOP*
CHBDL *COMBAT DF*

CIWES Migration Strategy



SSEE & ACCES

BGPHES ARS-ST & CHBDL

COMBAT DF (CDF)

COBLU
--OUTBOARD
--DF ECP

Pre FY-93 FY-93 FY-94 FY-95 FY-96 FY-97 FY-98 FY-99 FY-00

PAWS, LMS, CCSS, CCSC → SSEE

NIPS, JOTS, TFCC, ACS, EWCM, POST, ATP → NTCS-A

SSEE, ADAS, ECPI → CDF

SSEE, CCOP → COMMON BSLNE

OB, DF ECP, SSEE → COBLU

SSEE, ARS-ST → BGPHES

COMMERCIAL-BASED OPEN-SYSTEM STANDARD INFORMATION PROCESSING AND DISTRIBUTION

JMCIS 98-DII/COE

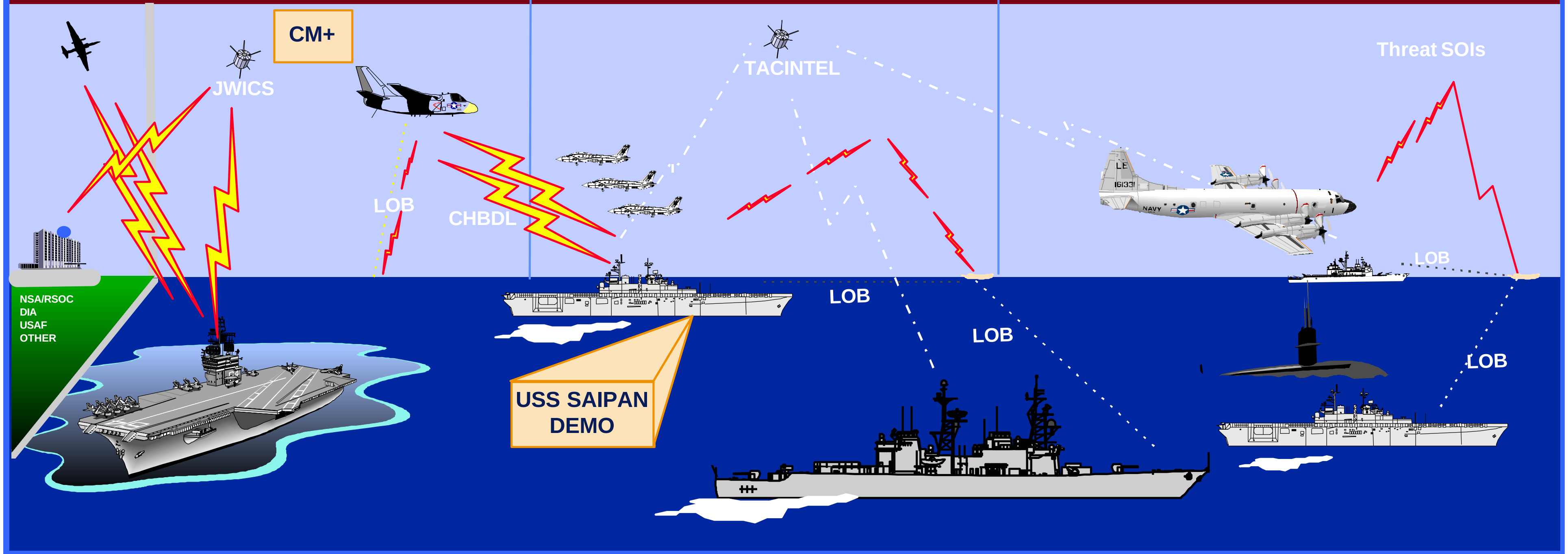
COMMON ARCHITECTURE

Shipboard SIGINT System Accomplishments

BGPHES Airborne Receiving System - Surface Terminal (BGPHES ARS-ST) / CHBDL

OUTBOARD and Combat DF

Ship's Signals Exploitation Equipment (SSEE) & Cryptologic Carry-On Program (CCOP)



BGPHES (ARS-ST)

- JOINT INTEROPERABILITY
- USAF NDI SOFTWARE
- JMCIS COMPLIANT
- CORE CAPABILITIES DEMONSTRATED
- SUCCESSFUL OPEVAL IN MARCH; MS III IN JUL

CHBDL

- NEWLY ACQUIRED BY PMW 163
- SUCCESSFUL OPEVAL IN MARCH
- MILESTONE DECISION REVIEW (MS III) COMPLETED 12 AUG

OUTBOARD / CDF

- DF ECP
- COBLU PHASE 0
- COBLU PHASE 1
- CDF MODERNIZATION
  - -- TAC - 3's, JMCIS
  - -- TECHNOLOGY INSERTION

SSEE / CCOP

- COMMON BASELINE
- VXI-BASED OPEN ARCH
- INCREMENTAL UPGRADES
- ACCELERATED DEPLOYMENTS
- INTEGRATED SCI LAN ARCH
- ACCES

IW-E Solutions Sought

- Reprogrammable Transceivers (i.e., Conventional, Frequency Hop (FH) Modes, etc., 2 MHz - 40 GHz)
- Real Time Multi-Lingual Automatic Voice Translators
- Faster/Cheaper DSP Multi-Chip Modules (MCM)
- Cheaper Data Links (> 10 MBPS, X, Ku Band)
- Real-Time Multi-Level Security for IW-E Data Distribution
- Software Reprogrammable Recognizers
- Programmable Intelligent Digital Electronics

NISE-East/NRaD
IW-D INDUSTRY BRIEF

Information Warfare - Defend

NISE-East/NRaD Primary Functions

- In-Service Engineering Activity (ISEA) (e.g., SPAWAR, NAVAIR, and NAVSEA Customer Base)
- Acquisition and ILS
- Security Services
- Software Life Cycle Support
- NRaD D87 INFOSEC Test Facility
- Installations

Industry Partnership
SPAWAR
'97

Information Warfare - Defend

ISEA Initiatives

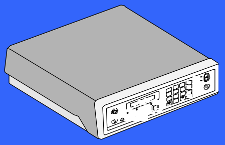
- Cryptographic Equipment Repair Program (CERP)
- INFOSEC Help Desk
- Secure Voice Support
- NSS Support
- CMI/PKI Support
- Key Management Support

Information Warfare - Defend

Acquisition and ILS

- Commercial Technology Purchased Through IDIQ, Umbrella, and General Schedule Contracts
  - NSS Products (e.g., Firewalls, Guards, Intrusion Detection Systems)
  - CMI/PKI Products (e.g., CAW Platforms)

- NDI Obtained Through Cooperation with the National Security Agency and Other Services
  - FASTLANE
  - KIV-7



- Competitive Procurements When Required for Specialized Products and Systems
  - KG-65
  - EIP/PEIP

SPAWAR '97 Industry Partnership

Information Warfare - Defend

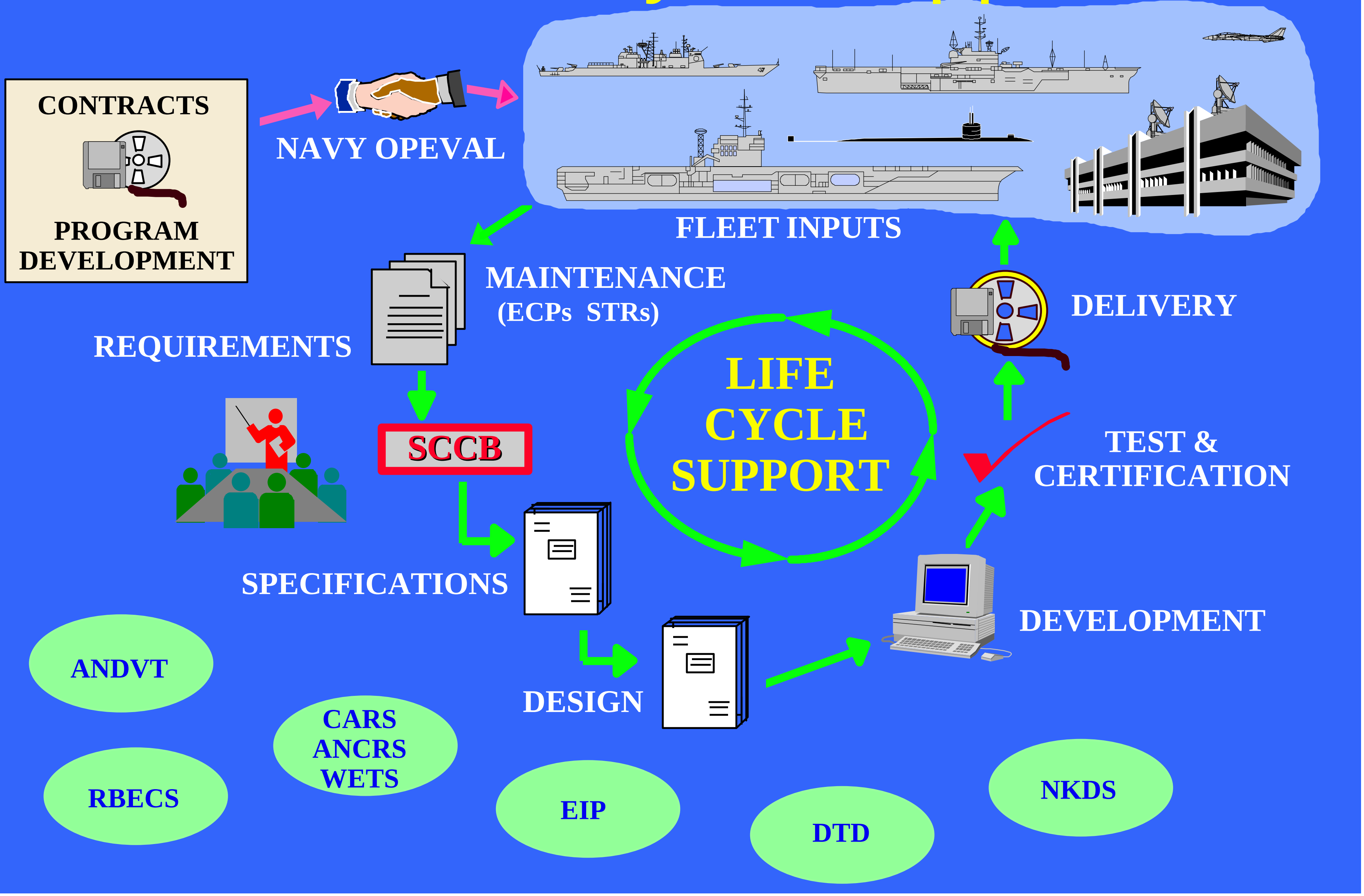
Security Services

- Education, Training and Awareness
- Fleet Workshops
- Engineering/Fielded System Support
- Certification and Accreditation

Industry Partnership
SPAWAR
'97

Information Warfare - Defend

Software Life Cycle Support



CONTRACTS

PROGRAM DEVELOPMENT

NAVY OPEVAL

FLEET INPUTS

MAINTENANCE
(ECPs STRs)

REQUIREMENTS

SCCB

SPECIFICATIONS

DESIGN

DEVELOPMENT

TEST & CERTIFICATION

DELIVERY

LIFE CYCLE SUPPORT

ANDVT

CARS
ANCRS
WETS

RBECS

EIP

DTD

NKDS

Information Warfare - Defend

NRaD D87 INFOSEC Test Facility

- Development, Integration, and Evaluation Laboratory to Support Information Security Products
- Networking Diverse Systems Within a Controlled Environment

NISE-East/NRaD
IW-E INDUSTRY BRIEF

Information Warfare - Exploit

NISE-East/NRaD Primary Functions

- ISEA/SSA/TDA
- Acquisition and ILS
- Integration & Production
- Installations Shore and Afloat

Information Warfare - Exploit

Recent IW-E Inroads

- Common Architecture “glidepath” Provided (C4ISR, JTA, JASA, MSA)
- Quick Reaction Capability (QRC) Becoming the Driving Requirement
- JMCIS/GCCS/DII Has Facilitated Common Core Functionality

Industry Partnership SPAWAR ’97

Information Warfare - Exploit

Ideas for the Future

- Intelligent Agents To Parse Databases
- Wideband A/D Converter, 100 Mega-Samples/sec, 14 Effective Bits, EMI Resistant, 40 v Peak-to-Peak
- Multi-channel Wideband Digital Downconverter, 10 MHz per Channel, Singleboard, VXI, S/W Programmable

Industry Partnership SPAWAR '97

Information Warfare - Exploit

Ideas for the Future (cont.)

- Reprogrammable Transceivers (conv/FH modes, 2M-40G)
- Smaller, Lighter, More Robust VXI-like Hardware
- Real-time Multi-lingual Automatic Voice translators
- Faster/Cheaper DSP Multi-Chip Modules(MCM)
- Signal Recognizers for Non-bauded Signals
- Co-channel Interference Techniques for Modern Signal Types (Freq Hoppers)

PD 16 Points of Contact

- PMW 161: Mr. Jack Stawiski
  - (619) 553-1145
  - stawiski@nosc.mil
- PMW 162: CDR Bob Zellmann
  - (301) 669-2313
  - zellmann@niwa.navy.mil
- PMW 163: Mr. Gary Wang
  - (703) 602-9549
  - wangg@smtp-gw.spawar.navy.mil
- NISE East Code 72: Mr. Gary Scott
  - (803) 974-5400
  - scottgr@niseeast.nosc.mil
- NRaD Code 7704: Mr. Lenny Coppenrath
  - (619) 553-5649
  - coppenl@nosc.mil

Industry Partnership
SPAWAR
'97